AN AUDIT A YEAR WILL KEEP YOU IN THE CLEAR

IT Summit
November 4th, 2009

Presented by: IT Internal Audit Team
Leroy Amos
Sue Ann Lipinski
Suzanne Lopez
Janice Shelton

WHY WE'RE HERE…

- We're here to provide a broad range of audit services designed to help our organization meet its objectives. One of our key roles is to monitor risks and ensure that the controls in place are adequate to mitigate those risks.
- We can help you comply with legislation and federal regulations within your agency.

HOW WE CAN HELP YOU…

- We’ll make an objective assessment of your operations, and share ideas for best practices.
- We’ll provide counsel for improving controls, processes and procedures, performance, and risk management.
- We’ll deliver competent consulting, assurance, and facilitation services.

AUDIT ENGAGEMENTS

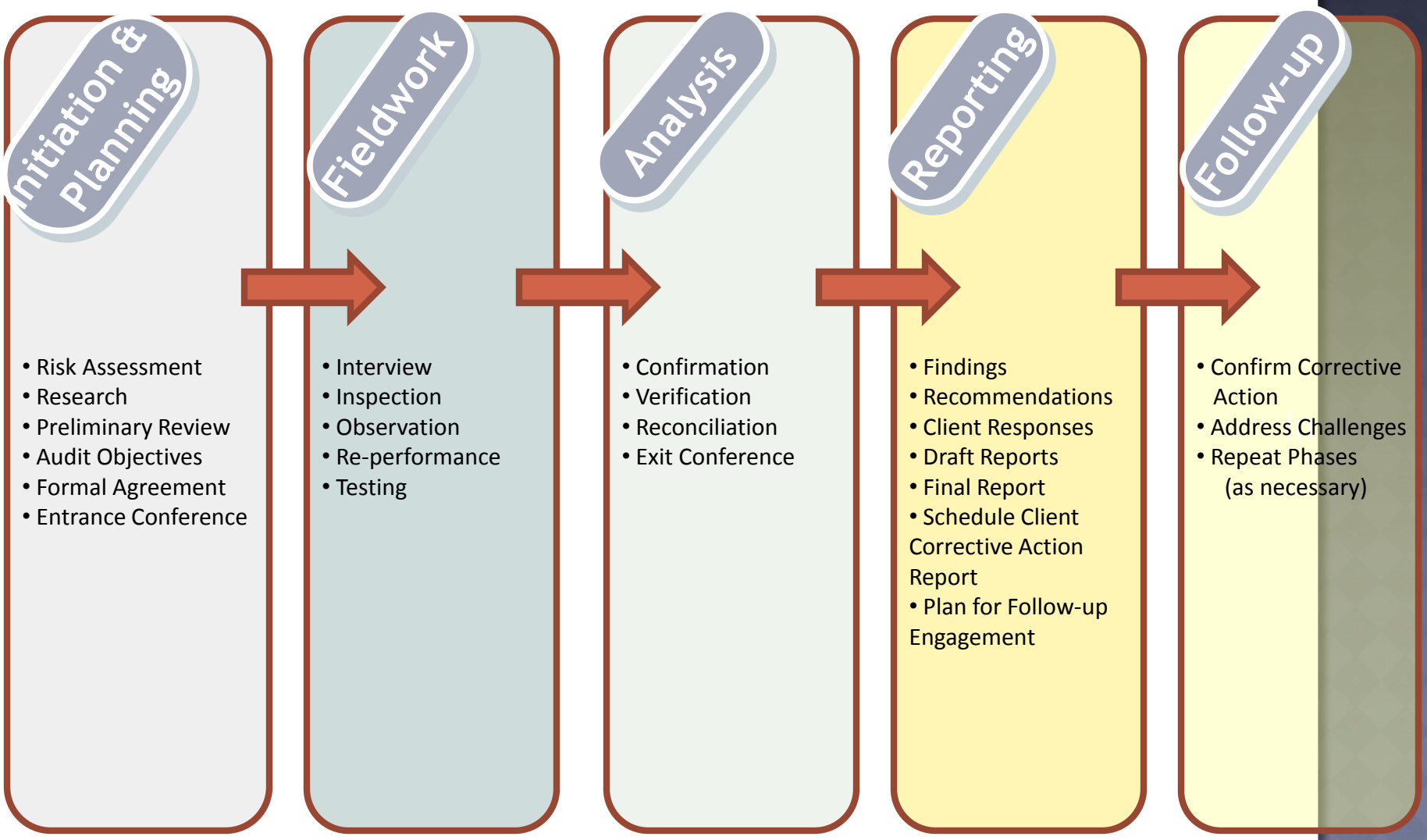
Three Types of Audits:

1. Internal
    - Client Request
    - Mandatory
2. Self Assessment
3. Third Party (External)
    - Agency must contact OISC prior to audit engagement
    - OISC will coordinate with third-party auditors

WHAT WE AUDIT

- Networks
- Desktop Practices
- Servers
- Mobile Devices and Media
- Data Centers/Facilities
- Business and Technical Processes
- Application Controls
- Policy and Procedure Compliance
- Other

INFORMATION SECURITY AUDIT PHASES



COMMON FINDINGS

- Unattended Workstations
- Password Sharing
- Weak Passwords
  http://www.microsoft.com/protect/fraud/passwords/checker.aspx
- Data Classification
- Confidentiality
- Lack of Policies and Procedures
- Account Management

AUDIT POLICY

- WVOT-PO1008 - Information Security Audit Program policy - issued: August 1, 2009
- http://www.technology.wv.gov/SiteCollectionDocuments/ISAP.pdf

CONFIDENTIALITY

- “All WVOT IT Auditors are bound by confidentiality standards and are required to sign the DOA Confidentiality Statement annually.”
- “Information collected during an audit will only be used for official purposes. This includes the proper handling of sensitive or classified information or resources.”

(*WVOT-PO1008, Information Security Audit Program*)

CONFIDENTIALITY *(CONTINUED)*

- "Delivery of engagement findings and recommendations will be limited to the CTO, the CISO, the client Director, and other parties as authorized."
- "The Information Security Audit Program will only release engagement findings and recommendations to additional entities under the following circumstances: by request from the audit client, for peer review, and/or under order of subpoena."

(*WVOT-PO1008, Information Security Audit Program)*

TEAMMATE SOFTWARE

- What is it?
  - System that maintains audit work papers, templates, reports, and other artifacts.
  - Necessary to achieve IT audit accreditation.
- How will it benefit the client?
  - Enable auditors to share information with the client in a secure manner.
  - Facilitate the tracking of follow-up actions.
  - Help auditors to identify common high risk findings.
  - Maintain an electronic client audit history

AUDIT WEBSITE

- Soft Launch Date – October 26, 2009
- Content
  - Explanation of the audit process
    - Audit Types
    - Audit Phases
  - Auditor and Client Responsibilities
  - FAQ
  - Code of Professional Ethics/Confidentiality
  - Audit team contact information
  - http://www.technology.wv.gov/security/ITAudit/Pages/default.aspx

West Virginia
Office Of Technology

- PRODUCTS & SERVICES
- About WVOT Internal Audit
- Types of Audits
- The Audit Process
- The Audit Life Cycle and Phases
- Auditor and Client Responsibilities
- Confidentiality
- Internal Controls
- FAQs
- Contact Information & IT Audit Links

IT Audit Services

About WVOT IT Internal Audit

The West Virginia Office of Technology (WVOT) Office of Information Security and Controls (OISC) is responsible for establishing, maintaining, and managing an objective and internally independent internal Information Security Audit Program.

This program serves the Executive Branch by examining, evaluating, and reporting on information technology (IT) applications, systems, operations, processes, and practices to provide reasonable assurance that security controls will:

- Safeguard information assets and protect privacy;
- Preserve the integrity and reliability of data;
- Function as intended to achieve the entity's objectives; and
- Comply with standards, policies, and regulations.

Audit efforts are focused on those operational areas presenting the highest degree of risk, as well as the greatest potential for benefit to the Executive Branch.

Internal Audit recommendations are designed to help Executive Branch agencies manage operations more efficiently, resulting in a more effective use of resources.

AUDIT PLAN

- SAS 70
- Account Management
- Data Center Audit
- End of Life Equipment Procedures
- Follow-Up Engagements
- Support for External Audits

WHAT YOU CAN EXPECT…

- Clarity
- Courtesy
- Credibility
- Consistency
- Competency
- Comprehension
- Communication

WHAT THIS MEANS TO YOU…

- You have, at your fingertips:
- A coach
- An advocate
- A risk manager
- A controls expert
- An efficiency specialist
- A problem-solving partner

WHAT THIS MEANS TO YOU…

- A safety net

HOW YOU CAN HELP US…

- Controls are everybody's business. This means we all need to work together toward mutual accountability for internal control. If you are aware of a control that's not working, let's put our heads together and come up with a way to make it better.

SCHEDULING AN AUDIT

- On an ad-hoc basis
- Post incident
- As a risk assessment
- All client requested engagements must be scheduled three (3) to six (6) months in advance

RISK ASSESSMENT EXERCISE

- **Access Controls** – enforcement of specified authorization rules based on positive identification of users.
- **Security of Assets** – physical and logical controls to protect data and technology resources from unauthorized use, modification, or disclosure.
- **Minimal Necessary and Limited Information Rule** – collection, use, and disclosure of information should be limited to an entity's legal authority and purpose.

RISK ASSESSMENT EXERCISE

- Answer Questions
- Check Your Answers
- Determine Your Risk Level

RISK ASSESSMENT EXERCISE

- Question 1: A
- Question 2: B
- Question 3: A or B
- Question 4: C
- Question 5: C
- Question 6: A
- Question 7: C

- Each correct answer is worth 1 point
- Score of 5 or above is low risk

QUESTIONS?

WVOT.ITAUDIT@WV.GOV

AUDITOR CONTACT INFORMATION

- Sue Ann Lipinski
  sueann.lipinski@wv.gov
- Leroy Amos
  j.leroy.amos@wv.gov
- Janice Shelton
  janice.l.shelton@wv.gov
- Suzanne Lopez
  suzanne.p.lopez@wv.gov